UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of: Information associated with accounts identified as "shootaswish95_" and "shootaswish59_" (SUBJECT ACCOUNTS) that is within the possession, custody, or control of Meta Platforms, Inc.	)	Case No. 2:22-MJ-02053

APPLICATION FOR WARRANT BY TELEPHONE PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

☑ Evidence of a crime;
☑ Contraband, fruits of crime, or other items illegally possessed;
☐ Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)	*Offense Description*
18 U.S.C. §§ 371, 922(g), 1028A, 1029, 1343, 1344	Conspiracy, Felon in Possession of a Firearm, Wire Fraud, Bank Fraud, Access Device Fraud, Aggravated Identity Theft

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

/s/ Christopher Lees
Applicant's signature
Christopher Lees, HSI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and State: Los Angeles, CA

Hon. Pedro V. Castillo, U.S. Magistrate Judge
Printed name and title

AUSA: Rachel N. Agress (x0487)

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the SUBJECT ACCOUNTS, identified as any accounts affiliated with the following Instagram usernames (collectively, SUBJECT ACCOUNTS): "shootaswish95_" (active from at least, but not limited to, October 14, 2021 through approximately on or about March 28, 2022) (SUBJECT ACCOUNT 1), "shootaswish59_" (active on from at least, but not limited to, April 26, 2021 through approximately on or about August 11, 2021), believed to be used by Meshack Samuels (SAMUELS), that is within the possession, custody, or control of Meta Platforms, Inc., a company that accepts service of legal process at 1601 Willow Road, Menlo Park, California, regardless of where such information is stored, held, or maintained.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURES

1. The warrant will be presented to personnel of Meta Platforms, Inc. (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other

sophisticated techniques. The review of the electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, limited to that which occurred between January 1, 2021 and the date of this warrant,[5] including:

i. All emails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account,

[5] To the extent it is not reasonably feasible for the PROVIDER to restrict any categories of records based on this date restriction (for example, because a date filter is not available for such data), the PROVIDER shall disclose those records in its possession at the time the warrant is served upon it.

draft messages, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each email or message (including the actual IP addresses of the sender and recipients of the emails), and any related documents or attachments,

ii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All data and information associated with the profile page of the SUBJECT ACCOUNT, including photographs, "bios," and profile backgrounds and themes;

iv. All communications or other messages sent or received by the SUBJECT ACCOUNT, including via Instagram Direct;

v. All user content created, uploaded, or shared by the SUBJECT ACCOUNT, all photos and videos uploaded by any user that have that user tagged in them, and all photos and videos "liked" or commented on by the user, including any comments made by the SUBJECT ACCOUNT on photographs, videos, or other content, as well as any metadata associated therewith, including, specifically, EXIF data;

vi. All photographs, videos, images, comments, captions, and hashtags, as well as any metadata associated therewith, in the user gallery for the SUBJECT ACCOUNT;

vii. All profile information, including but not limited to the user's website; a list of all of the people that

the user of the SUBJECT ACCOUNT follows on Instagram and all people who are following the user (i.e., the user's "following" list and "followers" list), as well as any "friends" of the user; "stories" by, tagged, or commented on by the user; places "liked" or visited by the user; "Follow" requests, including "Follow" requests sent to or from the SUBJECT ACCOUNT, and including Follow requests accepted or rejected; tags, including both who has been tagged on the SUBJECT ACCOUNT's profile and when the user of the SUBJECT ACCOUNT has been tagged in other users' profiles; notifications and notification settings of any kind; and information about the user's access and use of Instagram or third-party applications or "apps";

viii. A list of all users that the SUBJECT ACCOUNT has "unfollowed" or blocked;

ix. All "Active Sessions" information and activity logs for the account and all other documents showing the user's posts and other Instagram activities;

x. All location data associated with the SUBJECT ACCOUNT, or with photographs, videos, or other content, including geotags;

xi. All search history and web history for the user of the SUBJECT ACCOUNT, including records of Instagram searches and internet/web searches, and including web browsing that might occur outside of Instagram, but that Instagram is able to connect to the SUBJECT ACCOUNT when the SUBJECT ACCOUNT visit websites that are using Instagram's webpage "like" functionality;

xii. All records of the SUBJECT ACCOUNT's usage of the "Like" feature, including all Instagram posts and all non-Instagram webpages and content that the user has "liked" ("Likes on Others' Posts," "Likes on Your Posts from Others," and "Likes on Other Sites"); and

xiii. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or e-mail addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the following accounts:

(I) the SUBJECT ACCOUNTS.

ii. All privacy and account settings of the SUBJECT ACCOUNT, including past and present account status;

iii. All information about connections between the SUBJECT ACCOUNT and third-party websites and applications;

iv. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNTS described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

v. All information about the user's access and use of Instagram Checkout, or similar marketplaces;

vi. All information related to the SUBJECT ACCOUNT's membership in any groups, including the identity of other accounts in the same group, and information identifying any groups or organizational pages or accounts for which the SUBJECT ACCOUNT is an administrator;

vii. All push token or device token identifiers.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For the SUBJECT ACCOUNTS listed in Attachment A, the search team may seize:

a. All information described above in Section II.10.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371

(Conspiracy), 922(g) (Felon in Possession of a Firearm), 1343 (Wire Fraud), 1344 (Bank Fraud), 1029 (Access Device Fraud), and 1028A (Aggravated Identity Theft) (the "Subject Offenses"), namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNTS, including records about their identities and whereabouts;

ii. Information related to how and when the SUBJECT ACCOUNT was accessed or used;

iii. Records, documents, programs, applications, materials, or conversations relating to the trafficking of guns, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when guns, or ammunition were bought, sold, or otherwise distributed;

iv. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, possession or distribution of guns or ammunition;

v. Records, documents, programs, applications, pictures or materials referring to or containing credit and debit cards and accounts of any individual other than Meshack Samuels ("SAMUELS"), including related documents and records such as receipts or invoices;

vi. Records, documents, programs, applications, pictures or materials referring to or containing checks and cashier checks not in the name of SAMUELS;

vii. Records, documents, programs, applications, pictures or materials referring to or containing mail matter and shipping packages, opened or unopened, not addressed to or from SAMUELS;

viii. Personal identifying information of individuals other than SAMUELS, including social security numbers, other identifying numbers, dates of birth, addresses and telephone numbers, credit, gift debit card, or other account information, PINs, credit reports, and bank or financial institution, and records referring to or relating to such information;

ix. Records, documents, programs, applications, pictures or materials referring to or containing counterfeiting or manipulation of documents and identifications, such as the cutting-and-pasting of signatures, forging or copying passports, driver's licenses, and other forms of identification, identification-proportioned photographs of faces, letterheads, watermarks, seals and logos, including altered or counterfeited information itself;

x. Records, documents, programs, applications, pictures or materials referring to wealth and the movement of wealth since 2021 such as cryptocurrency accounts and transfers, other digital wealth storage and transfer methods including PayPal and Venmo, money orders, brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashier's checks, transactions involving prepaid cards, and/or financial documents related to depository bank

accounts, lines of credit, credit card accounts, real estate mortgage initial purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, renting or leasing of automobiles or real estate, or auto loans, and investments or showing or referring to purchases or transactions for more than $1,000;

xi. Records, documents, programs, applications, or materials pertaining to applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

xii. Documents, records and materials referring to or relating to law enforcement or bank investigations, accounts being closed or at risk of being closed, currency transaction reports, and manipulating transaction amounts to avoid scrutiny;

xiii. Records, documents, programs, applications, or materials regarding any tax-related records, filings, or correspondence for any individual other than SAMUELS.

xiv. Information relating to the location, storage, or concealment of cash, money instruments, virtual currency, or money equivalents; and

xv. Information relating to co-conspirators engaged in the SUBJECT OFFENSES, which could include information relating to their identities, whereabouts, communications, and methods of contact and communication.

b. All records and information described above in Section II.10.b.

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the service of this warrant. The PROVIDER shall send such information to:

Christopher Lees
Special Agent, Homeland Security Investigations
6319 Alondra Blvd.
Paramount, CA 90723
Phone Number: 562-371-7650
Email: christopher.r.lees@ice.dhs.gov

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant.

AFFIDAVIT

I, Christopher Lees, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with Homeland Security Investigations ("HSI") in Los Angeles, California and have been so employed since August 2020. I am currently assigned to the El Camino Real Financial Crimes Task Force, where I investigate matters concerning bank fraud, wire fraud, identity theft, money laundering, and other illegal financial transactions.

2. To become an HSI Special Agent, I completed 6 months of training at the Federal Law Enforcement Training Center in Brunswick, Georgia. During my employment as an HSI Special Agent, I have participated in several investigations related to narcotics smuggling, weapons trafficking, organized criminal activity, bank fraud, wire fraud, and other financial crimes. I have participated in various aspects of criminal investigations, including bank records analysis, telephone records analysis, electronic surveillance, physical surveillance, search warrants, arrests, and reviewing evidence from digital devices. I have also spoken to many law enforcement agents regarding their experience in investigating financial crimes, and interviewed defendants, and witnesses who had personal knowledge regarding the methods used to commit a variety of financial crimes.

II. BACKGROUND

3. I make this affidavit in support of an application for a warrant for information associated with the accounts

identified as affiliated with the following Instagram usernames (collectively, SUBJECT ACCOUNTS): "shootaswish95_" (active from at least, but not limited to, October 14, 2021 through approximately on or about March 28, 2022) (SUBJECT ACCOUNT 1), "shootaswish59_" (active on from at least, but not limited to, April 26, 2021 through approximately on or about August 11, 2021) (SUBJECT ACCOUNT 2), believed to be used by Meshack Samuels ("SAMUELS"), that is stored at premises controlled by Meta Platforms, Inc. (the "PROVIDER"), a provider of electronic communication and remote computing services, headquartered at 1601 Willow Road, Menlo Park, California 94025.[1]

4. The information to be searched is described in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(d)[2] to require the

---

[1] Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

[2] The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which does not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c)(1), (c)(2). To obtain additional records and other information--but not

PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

5. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNTS constitutes evidence, contraband, fruits, or instrumentalities of criminal violations 18 U.S.C. §§ 371 (Conspiracy), 922(g) (Felon in Possession of a Firearm), 1343 (Wire Fraud), 1344 (Bank Fraud), 1029 (Access Device Fraud), and 1028A (Aggravated Identity Theft) (the "Subject Offenses").

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there

---

content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c)(1)(B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment B paragraph II.10.a.) as well as subscriber records and other records and information that do not contain content (see Attachment B paragraph II.10.b.).

is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

III. SUMMARY OF PROBABLE CAUSE

7. As early as approximately March 2021, SAMUELS has routinely posted public pictures, videos and stories on Instagram, utilizing the SUBJECT ACCOUNTS, of himself in possession of large amounts of currency, suspected stolen or fraudulent checks, as well as deposit receipts and slips not in his name from various financial institutions. In public Instagram posts, SAMUELS also urged individuals to join his Telegram chat group for a fee, that will teach them how to make quick money off of banks, and also solicited third parties with bank accounts at specific financial institutions. Based on my training and experience, I know that fraudsters frequently solicit "clean" bank accounts from third parties that are less likely to be flagged by banks, to deposit stolen or fraudulent checks and withdraw the funds.

8. SAMUELS also routinely posted public pictures, videos and stories on Instagram, of himself in possession of firearms. SAMUELS is a convicted felon.

9. On August 29, 2021, pursuant to an independent traffic stop and a search of SAMUEL's car, Costa Mesa Police Department

seized blank checks and a credit card in names other than SAMUELS' or his passenger, J.G., approximately $8,855.00 in cash from the center console, and a loaded pistol from SAMUELS' underwear. On March 22, 2022, SAMUELS was indicted for being a felon in possession of a firearm and ammunition in Case No. 22-CR-00030.

10. On March 28, 2022, law enforcement executed a federal search warrant at SAMUELS' residence, and seized five firearms, significant numbers of debit cards and checks not in the names of SAMUELS or the other residents, multiple legers containing identifying information for dozens of individuals, along with bank account numbers, printing and scanning materials, a money counter, and approximately $45,000 in bulk cash, as well as multiple digital devices, among other things.

IV. STATEMENT OF PROBABLE CAUSE

11. Based on my review of investigative reports and notes, bank statements, preserved public Instagram messages, witness statements, my discussions with other law enforcement officers working on this investigation, and other evidence, I learned the following information:

A. Identification of SAMUELS' Social Media Accounts

12. Local law enforcement agencies in New York and Florida brought SAMUELS' Instagram profiles to my attention, registered under the usernames "shootaswish95_" (SUBJECT ACCOUNT 1) and "shootaswish59_" (SUBJECT ACCOUNT 2), and informed me that they have been monitoring and preserving SAMUELS' public social media

posts on the SUBJECT ACCOUNTS dating back to approximately February 26, 2021 (following SAMUELS' release from custody on state charges in Florida), in conjunction with a broader investigation into SAMUELS' ongoing criminal activity.[3]

13. On or about March 22, 2022, the Honorable John E. McDermott, United States Magistrate Judge of the Central District of California, authorized a federal warrant to search digital devices seized from SAMUELS' vehicle following his arrest on August 29, 2021, Case No. 2:22-MJ-01142. During my review of those devices, believed to belong to SAMUELS, I discovered screenshots of activity by SUBECT ACCOUNT 2.

14. Based on metadata from public Instagram posts on the SUBJECT ACCOUNTS preserved by local law enforcement agencies in New York and Florida, and metadata from screenshots of SUBJECT ACCOUNT 2 activity on SAMUELS' devices, SAMUELS used SUBJECT ACCOUNT 2 from at least, but not limited to, April 26, 2021 through approximately on or about August 11, 2021, and SUBJECT ACCOUNT 1 from at least, but not limited to, October 14, 2021 through approximately on or about March 28, 2022, the date of his arrest on federal charges in this district in Case No. CR 20-00030-CJC, to post firearm-related content, and to recruit associates to commit financial crimes.

---

[3] On October 26, 2021, a state warrant on SUBJECT ACCOUNT 1 was authorized by the Honorable Judge John Ziny of the Superior Court of California, Orange County. The government relies solely on public posts in this application and is not relying on any returns from that state warrant herein.

15. Based on my training and experience, individuals who are engaging in criminal activity may shut down social media accounts to evade detection by law enforcement. When they do so, they will frequently open up other accounts with similar usernames, so that customers and other criminal associates can easily find their new username, including opening new usernames under the old account. Based on what I have learned and my training and experience, I believe that SAMUELS consecutively used SUBJECT ACCOUNT 1, SUBJECT ACCOUNT 2 and potentially other linked accounts with similar names, from around the time of his release from incarceration on or about February 26, 2021 through is arrest on federal charges on or about March 28, 2022.

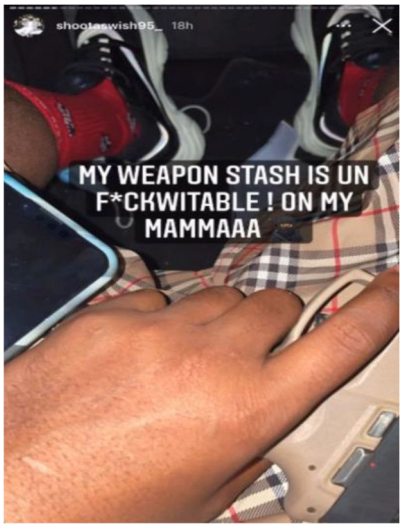
16. I have reviewed the public posts preserved by New York and Florida law enforcement as well as additional public posts on that account. I recognize SAMUELS in many of the photos posted to the Instagram Account from my interactions with him on March 28, 2022, the date of his arrest on federal charges.

B. SAMUELS Posts Himself With Multiple Firearms On Social Media

17. SAMUELS made numerous public posts of SAMUELS exhibiting semiautomatics pistols, despite his status as a convicted felon.

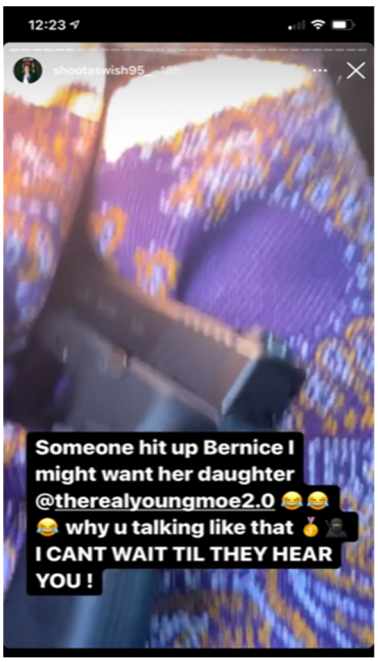
18. For example, on or about October 14, 2021, and October 16, 2021, SAMUELS posted the following photos to SUBJECT ACCOUNT 1, where he was in possession of a tan and black firearm:

19. On or about October 24, 2021, SAMUELS posted a photo to SUBJECT ACCOUNT 1 of what looked to be the same firearm from his previous post in his possession:



20. In a photo posted by SAMUELS to SUBJECT ACCOUNT 1 on or about November 11, 2021, SAMUELS appears to be posing with large amounts of cash while wearing two semiautomatic pistols tucked in his pockets, and the one in his right pocket appears to be tan and black:

21. On or about February 10, 2022, SAMUELS posted the following photo to SUBJECT ACCOUNT 1, showing a firearm:



22. On or about February 11, 2022 SAMUELS posted a photo to SUBJECT ACCOUNT 1 in which he is posing in front of a mirror with two semi-automatic pistols protruding from both front jeans pockets. This picture is captioned by the comment "Lol I just wake up n put it on!":

23. On or about March 1, 2022, SAMUELS posted a video to SUBJECT ACCOUNT 1, of him waiving what appears to be a black and tan firearm.

C. Criminal History

24. I reviewed SAMUELS' criminal history records and learned that SAMUELS has previously been convicted of the following felony crimes punishable by a term of imprisonment exceeding one year:

a. On or about August 30, 2016, a first-degree felony violation of Florida Statutes Sections 784.07(2)(d): Aggravated Battery on a Law Enforcement Officer, 782.065: Attempted Murder of a Law Enforcement Officer, 777.04: Attempt, 775.0823: Violent Offense Committed Against Law Enforcement Officer, and 775.087: Aggravated Battery; and a third-degree felony violation of Florida Statutes Section 316.1935(1): Fleeing or Attempting to Elude a Law Enforcement Officer, in the Miami-Dade County Court, Case Number F15-007045.

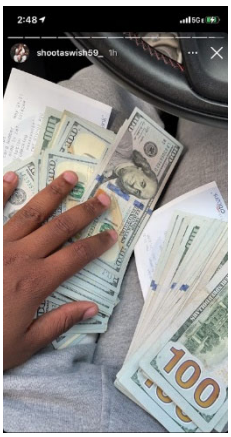
b. On or about August 4, 2020, a second-degree violation of Florida Statutes Section 790.23(1): Possession of a Firearm, Weapon or Ammunition by a Convicted Felon in the Miami-Dade County Court, Case Number F20-004582.

D. SAMUELS Posts About Committing Financial Fraud on Social Media Using SUBJECT ACCOUNTS 1 and 2

25. On the SUBJECT ACCOUNTS, in numerous public posts, SAMUELS indicated that he was making money off of banks, invited his Instagram followers to join a Telegram chat group for a fee named "WINNING OUR ONLY OPTION", that will teach them how to make quick money off of banks, and also solicited third parties with bank accounts at specific financial institutions. Based on

my training and experience, I know that fraudsters frequently solicit "clean" bank accounts from third parties that are less likely to be flagged by banks, to deposit stolen or fraudulent checks and withdraw the funds.

26. For example, on an unknown date, SAMUELS posted on SUBJECT ACCOUNT 2 to his story two images of stacks of $100 bills and three Citibank deposit slips, two of which were dated May 21, 2021. One of the images contained a caption stating



that SAMUELS "got the citi hot," which I understand, based on my training and experience and the other posts by SAMUELS, refer to fraud on Citibank.

//

//

//

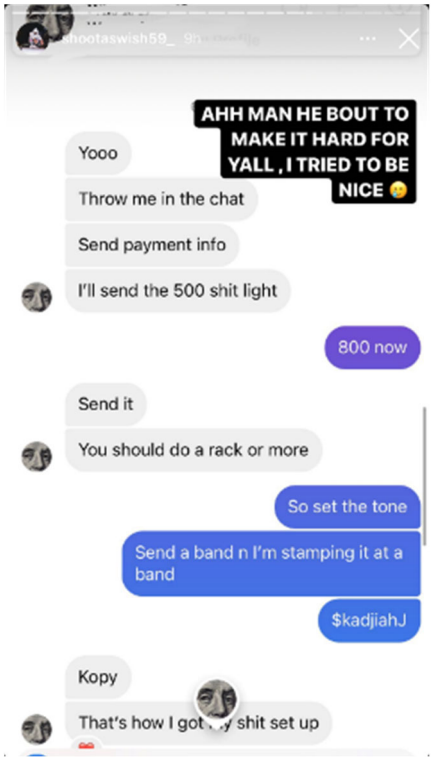
//

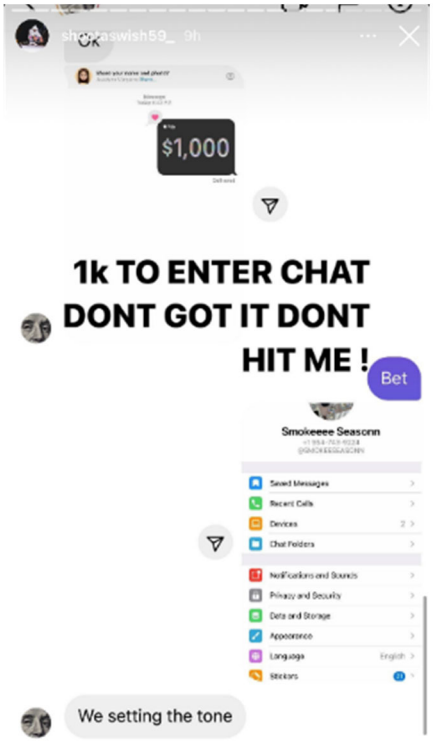
//

//

//

27. On or about June 30, 2021, SAMUELS posted to SUBJECT ACCOUNT 2 several screenshots from his Telegram chat stating that the entry fee to the chat group had gone up from $500 to $800 to $1,000:





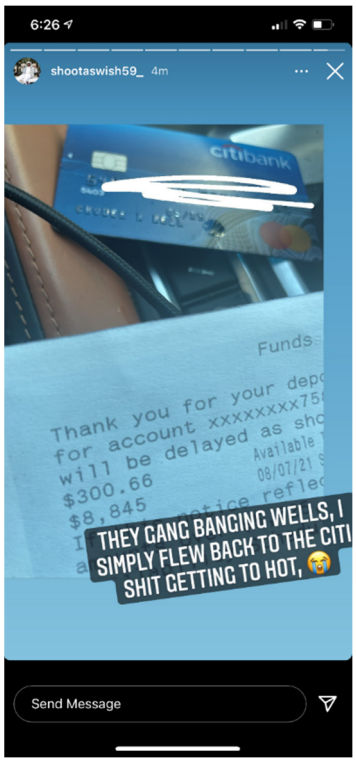
28. On or about August 11, 2021, SAMUELS posted on SUBJECT ACCOUNT 2 a screenshot of a redacted Wells Fargo receipt dated July 12, 2021, listing a $7,000 check deposit into a bank account under the name "M.," referencing a "Wells drip" which I

understand, based on my training and experience and the context of other posts by SAMUELS, to refer to fraud on Wells Fargo.

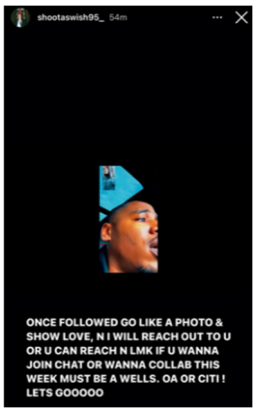
29. On or about August 11, 2021, SAMUELS reposted a story from another account "baccend_sleeze" on SUBJECT ACCOUNT 2. "baccend_sleeze" was advertising for individuals with Citibank accounts, and said in his/her post, stated that the individual affiliated with SUBJECT ACCOUNT 2 (SAMUELS) had a "cheat code."

30. For example, on or about August 10, 2021, SAMUELS posted on SUBJECT ACCOUNT 2 to his story an images of a Citibank withdrawal slip dated August 7, 2021, and a Citibank card not in SAMUELS's name, containing the caption "They gang banging Wells,

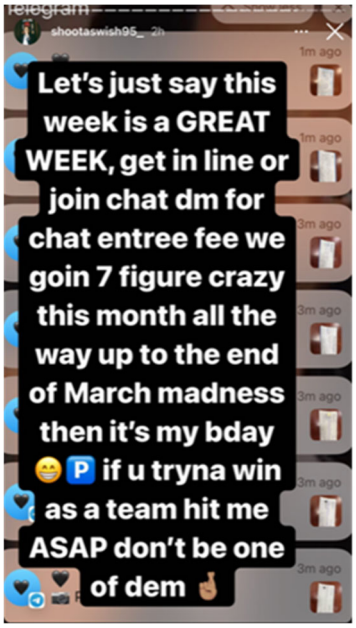
I simply flew back to the Citi[,] shit getting to [sic] hot," which I understand, based on my training and experience and the other posts by SAMUELS, to refer to the fact that while other individuals are committing fraud on Wells, SAMUELS is committing fraud on Citibank.



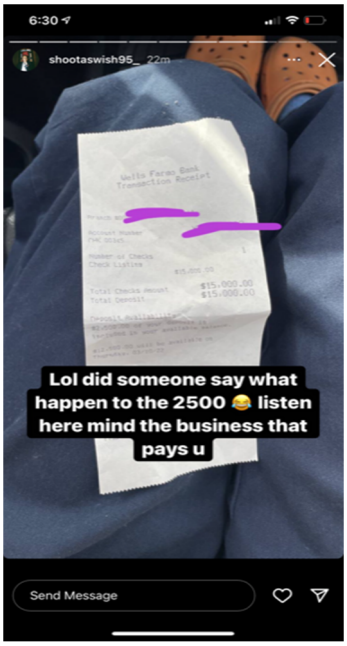
31. On or about February 11, 2022, SAMUELS posted on SUBJECT ACCOUNT 1 that all he needed to collaborate is a Wells Fargo or Citibank account:



32. On or about February 15, 2022, SAMUELS publicly posted to SUBJECT ACCOUNT 1 a screenshot from his telegram chat and said people should contact him regarding the entry fee showing an entry fee for a chat. In the background appear to be images of receipts related to the suspected bank fraud scheme:



33. On or about March 9, 2022, SAMUELS posted on SUBJECT ACCOUNT 1 a screenshot of a redacted Wells Fargo receipt listing a $15,000 check deposit as follows:



E. SAMUELS' History of Engaging in Financial Fraud

34. I have learned the following regarding SAMUELS' criminal history from New York and Florida law enforcement agencies: when SAMUELS was arrested at a hotel in 2015 in connection with his eventual 2015 conviction referenced in paragraph 14(a), fraudulent credit cards and identification were found in the hotel room; and in conjunction with his 2020 arrest, SAMUELS led the police on a high-speed chase in a Mercedes-Benz C300 and was involved in a number of crashes, before ultimately running a red light and striking another vehicle, leaving the car inoperable, and after SAMUELS fled the scene, a search of the vehicle revealed blank checks and other forgery instruments inside.

F. Pursuant to Traffic Stop on August 29, 2021, SAMUELS is Found With a Loaded Firearm and Instruments Indicative of Fraud, and Indicted on 922(g) Charges

35. On August 29, 2021, an officer with the Costa Mesa Police Department("CMPD") initiated a traffic stop on a black BMW for littering and expired registration. Upon contact SAMUELS repeatedly provided a false name and date of birth to the officer, and appeared to have photographs of multiple identification cards on his phone. SAMUELS was also reaching his hands down and moving around, and so was relocated to the curb, uncuffed, for officer safety. Finally, SAMUELS admitted to providing a false name, provided his real name and gave the officer verbal consent to search his vehicle.

36. During the search, the officer located blank checks in names other than SAMUELS or the passenger, J.G., including six checks that were blank except for a signature, checks with an address in San Diego, checks issued by Well Fargo in Florida, New Jersey and California, two filled-out check in names other than SAMUELS or J.G., a moneygram in names other than SAMUELS or J.G., and a cashiers check with a remitter name other than SAMUELS or J.G. There was also a Citibank credit card in a name other than SAMUELS or J.G., and approximately $8,855.00 cash in the center console. SAMUELS denied ownership or knowledge of the checks or Citibank card in the vehicle, but said the cash belonged to him.

37. SAMUELS was arrested and resisted officers' attempts to conduct a search of his person. During the pat-down search, officers found and recovered a black and silver Ruger LCP .380

caliber semi-automatic pistol bearing serial number 374-81336, from SAMUELS' underwear. The firearm was loaded with four rounds of .380 Auto S&P ammunition: a live round in the chamber and three rounds in an inserted magazine.

38. A Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), Firearms Interstate Nexus Expert examined the handgun seized from SAMUELS and confirmed that the handgun was manufactured outside of the State of California. Because the handgun was found in California, I believe that it traveled in and affected interstate and/or foreign commerce.

39. On March 22, 2022, SAMUELS was indicted for being a felon in possession of a firearm and ammunition in Case No. 22-CR-00030.

G. Five Firearms and Items Indicative of Fraud Found during Search of SAMUELS' Residence and Car

40. On March 22, 2022, the Honorable John E. McDermott, United States Magistrate Judge, Central District of California, authorized a federal search warrant on SAMUELS' residence and car in Placentia, California, Case Nos. 2:22-MJ-01139, 2:22-MJ-01140. The warrant was executed on March 28, 2022. At the house, law enforcement seized five semi-automatic pistols (with ammunition and magazines).

41. Based on my review of SAMUELS' Instagram posts on the SUBJECT ACCOUNTS and photos of the recovered firearms, at least five of the firearms seized during the search warrant matched the firearms previously posted in photographs and videos on the

SUBJECT ACCOUNTS, recognizable based on make, model, caliber and color.

42. Law enforcement also seized approximately $44,777 in cash, eight digital devices, numerous bank debit and credit cards not in the name of SAMUELS or any of the other residents, numerous commercial, personal and Treasury checks nor in the name of SAMUELS or any of the other residents, numerous pages of blank check card stock in varying sizes and colors, transaction deposit receipts and slips from numerous financial institutions not in the names of SAMUELS or any of the other residents, five notebooks ledgers containing names, dates of birth, social security numbers, bank account numbers, routing numbers, phone numbers, and addresses, a bill counter and a magnetic strip card reader, and paperwork and mail in the name of SAMUELS and an individual, S.J., indicating that they were the residents. In addition, law enforcement seized handwritten notes with username and passwords to numerous social media accounts written on them.

43. Also found in the residence, but not seized, were luxury high end watches and jewelry, high end designer clothes and shoes, high end designer purses and handbags, as well as high end designer sunglasses.

44. From SAMUELS' car, law enforcement seized numerous checks not in the name of SAMUELS or the residents, Wells Fargo deposit transaction receipts not in the name of SAMUELS or the residents, an International Driver's License in the name of S.J., and an HP Envy printer/scanner.

45. Other than what has been described herein, to my knowledge the United States has not attempted to obtain the contents of the SUBJECT ACCOUNTS by other means.

V. SERVICES PROVIDED BY INSTAGRAM

46. Based on a review of information provided by Meta Platforms, Inc. and Instagram regarding Instagram's services, information provided by other law enforcement officers, and/or my training and experience, I am aware of the information contained in this section of the affidavit regarding Instagram.

47. Instagram is a free-access social networking service owned by Meta Platforms, Inc. ("Meta"), accessible through its website and its mobile applications, that allows subscribers to acquire and use Instagram accounts, like the SUBJECT ACCOUNTS, through which users can share messages, multimedia, and other information with other Instagram users and the general public.[4]

48. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address, telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

49. Meta also collects and retains information about how each user accesses and uses Instagram. This includes

[4] Meta also owns other social networking and communications platforms, including Facebook and WhatsApp.

information about the IP addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, as well as session times and durations. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a SUBJECT ACCOUNT.

50. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

51. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and other third-party websites and mobile apps.

52. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

53. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

54. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

55. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos.

Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

56. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

57. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

58. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator

chooses to send the video to IGTV, Instagram's long-form video app.

59. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

60. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on the Facebook platform and other associated websites and apps. Meta collects and retains payment information, billing records, and transactional and other information when these services are utilized.

61. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to

generate related updates from Instagram. Meta retains records of an Instagram user's search history and followed hashtags.

62. Meta also collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

63. Meta also uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. In my training and experience, this data can provide information that can also be used to identify the user(s) of a SUBJECT ACCOUNT.

64. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

65. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers,

email addresses, full names, privacy settings, email addresses, and profile bios and links).

66. In my training and experience, the stored communications and files described above connected to a SUBJECT ACCOUNT may provide direct evidence of the offenses under investigation and may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT. In addition, emails, instant messages, internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

67. In my training and experience, a user's account activity, logs, stored electronic communications, and other data retained by Meta can also be used to identify the user(s) of a SUBJECT ACCOUNT. For example, subscriber information, IP address logs, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crimes under investigation.

VI. BACKGROUND ON THE SEIZURE OF DIGITAL EVIDENCE FROM THE PROVIDER

68. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at

a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account, including the email addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with a SUBJECT ACCOUNT with the date restriction included in Attachment B for review by the search team.

69. Relatedly, the government must be allowed to determine whether other individuals had access to a SUBJECT ACCOUNT. If

the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

70. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

71. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court,

regardless of where the PROVIDER has chosen to store such information.

72. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

73. I make that request because I believe it might be impossible for a provider to authenticate information taken from a SUBJECT ACCOUNT as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search team and confirm that it was a business record of the provider taken from a SUBJECT ACCOUNT.

74. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is

incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

VII. CONCLUSION

75. Based on the foregoing, I request that the Court issue the requested warrant. The government will execute this warrant by serving the warrant on the PROVIDER. Because the warrant will be served on the PROVIDER, which will then compile the requested records at a time convenient to it, reasonable cause exists the permit the execution of the requested warrant at any time in the day or night.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 24th day of May, 2022.

HONORABLE PEDRO V. CASTILLO
UNITED STATES MAGISTRATE JUDGE